

REMARKS

Claims 38-73 are pending in the present application. Claims 38-41 are the independent claims.

Claims 38-48, 50-56, 58-64, and 66-72 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,499,294 (Friedman), and Claims 49, 57, 65, and 73 stand rejected under 35 U.S.C. § 103(a) as being obvious over Friedman. Applicants respectfully traverse those rejections for the following reasons.

As recited in independent Claim 38, the present invention is directed to an apparatus for generating data used for checking whether or not an encoded digital image is changed. As discussed in the Background section of the present application, a conventional system for performing the function using public key cryptography. In particular, digital data is compressed using a hash function, and the result of the hash function is encrypted with a private key to obtain digital signature data. The digital data and the digital signature are sent to a receiving side, where the public key is used to decrypt the hash function data. The received digital data is compressed using the same hash function, and if the result matches the decrypted hash function data received with the digital data, the data is unchanged. *See* page 2, line 9 - page 3, line 7 of the specification.

A drawback of the conventional system, however, is that a great deal of time and processing power are required to perform public key encryption and decryption. The present invention as recited in independent Claim 38 is directed to addressing that drawback, and it does so by providing an apparatus that includes, *inter alia*, the features of performing a predetermined calculation using an encoded digital image and confidential

information, and generating additional data using a result of the predetermined calculation. As a result of these features, the integrity of digital data (i.e., whether the data has been altered) can be checked more quickly and with less processing. In particular, by first performing a predetermined calculation using an encoded digital image and confidential information, and then generating additional data using the result of that calculation, the use of public key encryption/decryption can be avoided while still reliably checking the integrity of the digital image data.

Applicants submit that the cited art fails to disclose or suggest at least the above-mentioned feature. The Examiner asserts that in Friedman (i) the predetermined calculation is the encrypted hash and the confidential information is the private key (citing Col. 4, lines 34-36 and 55-67) and (ii) the additional data that is generated is the digital signature, which is generated from the predetermined calculation of the hash (citing Col. 5, lines 56-60). Applicants respectfully disagree and submit that Claim 38 cannot reasonably be read on the disclosure of Friedman.

Friedman merely discloses a conventional system as disclosed in the Background section of the present application (and as discussed above). In particular, Applicants submit that Friedman discloses performing a hash function on image data (which is not disclosed as being encoded) and “using the camera’s unique private key . . . to encrypt a hash of the captured image file . . . for creating an encrypted image hash, thus producing a digital signature.” (Col. 5, lines 58-62.) If the encrypting of the image hash using the private key in Friedman is construed to be a predetermined calculation on encoded image data using confidential information, then Friedman does not disclose or

suggest generating additional data using the result of the predetermined calculation. In Friedman, the hash encrypted with the private key is the digital signature, and there is no further step. By asserting that the additional data that is generated in Friedman is the digital signature, Applicants respectively submit that the Examiner appears to misconstrue Friedman as having some further process to produce the digital signature, which is not the case.

For the foregoing reasons, Applicants submit that Friedman does not disclose or suggest at least the above-mentioned features of Claim 38.

Independent Claim 40 is a corresponding method claim and recites similar features.

As recited in independent Claim 39, the present invention includes, among others, the features of inputting an encoded digital image with first additional data, performing a predetermined calculation using the encoded digital image and confidential information, and generating second additional data using a result of the predetermined calculation.

Applicants submit that Friedman also fails to disclose or suggest at least the above-mentioned features. The Examiner asserts that in Friedman (i) the first additional data is the digital image file (citing Col. 6, lines 10-15), (ii) the calculation unit calculates the encryption of the hash using the private key as the confidential information (citing Col. 5, lines 52-67), and (iii) the second additional data is the digital signature (citing Col. 5, lines 56-60). Applicants respectfully disagree.

The Examiner's assertion that the first additional data in Friedman can be construed to be the digital image is incorrect, because Claim 39 recites inputting the encoded digital image *with* first additional data. Therefore, the digital image cannot be the first additional data that is input with itself. In Friedman, the authentication system 20 inputs the digital image file, the digital signature, and the public key for use in performing authentication.

Regarding the predetermined calculation and the generation of second additional data, the Examiner is citing portions of Friedman that relate to the formation of the digital signature in the camera, not to the use of the digital signature in the authentication system 20 to determine whether the digital image has been changed.

Accordingly, Applicants submit that Friedman fails to disclose or suggest at least the above-mentioned features of Claim 39. Independent Claim 41 is a corresponding method claim that recites similar features.

For the foregoing reasons, Applicants submit that this application is in condition for allowance. Favorable reconsideration, withdrawal of the rejections set forth in the above-mentioned Office Action, and an early Notice of Allowance are requested.

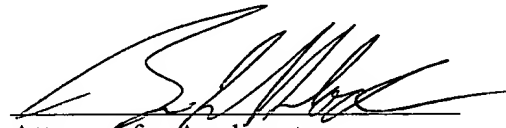
REQUEST FOR PERSONAL INTERVIEW

It appears to Applicants that a personal interview may be beneficial for the advancement of prosecution. Accordingly, the Examiner is requested to contact Applicants' undersigned representative to schedule an interview, at which the disclosure of

Friedman and the differences between that patent and the claimed invention can be discussed.

Applicants' undersigned attorney may be reached in our Washington, DC office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'B. L. Klock', is written over a horizontal line.

Attorney for Applicants
Brian L. Klock
Registration No.36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/lmj
DC 171859v1